Re-Socializing Online Social Networks

Michael Dürr[1] and Martin Werner[1]

Mobile and Distributed Systems Group
Ludwig Maximilian University Munich, Germany
{michael.duerr,martin.werner}@ifi.lmu.de,
Web: http://www.mobile.ifi.lmu.de/

Abstract. Recently the rapid development of *Online Social Networks* (OSN) has extreme influenced our global community's communication patterns. This primarily manifests in an exponentially increasing number of users of *Social Network Services* (SNS) such as Facebook or Twitter. A fundamental problem accompanied by the utilization of OSNs is given by an insufficient guarantee for its users informational self-determination and an intolerable dissemination of socially incompatible content. This reflects in severe shortcomings for both the possibility to customize privacy and security settings and the unsolicited centralized data acquisition and aggregation of profile information and content.
Considering these problems, we provide an analysis of requirements an OSN has to fulfill in order to guarantee compliance with its users' privacy demands. Furthermore, we present a novel decentralized multi-domain OSN design which complies with our requirements. This work significantly differs from existing approaches in that it, for the first time, allows for a technically mature mapping of real-life communication patterns to an OSN. Our concept forms the basis for a secure and privacy-enhanced OSN architecture which eliminates the problem of socially incompatible content dissemination.

Key words: Availability, Informational Self-Determination, Online Social Networks, Privacy, Trust

1 Introduction

Online Social Networks (OSN) represent a means to map communication flows of real-life relationships to existing computer networks such as the Internet. Almost all successful *Social Network Service* (SNS) providers like LinkedIn, Xing, MySpace, Facebook, Google Buzz, YouTube, Twitter, and others, operate their services commercially and in a centralized way. Although many of these SNSs address selected user groups (Xing and LinkedIn target at business professionals, MySpace primarily addresses private and leisure relationships), they all have in common that their users utilize these OSNs for communication, information sharing, and data exchange. Shared information is manifold and ranges from private and public contact details, sensitive personal profile information (comprising date of birth, marital status, political, religious and sexual orientation,

hobbies and personal interests, education history, to list just a few) to music, images, photos, videos, and other multimedia content.

SNSs provide a convenient way to shift a multitude of everyday communication, information access, and information retrieval operations to a single, centralized platform. The increasing number of OSN memberships reflects their immense popularity. Facebook alone grows at a rate of over 700.000 users a day [Smi09] and currently holds 400 million active users, i.e. users who have returned to the site in the last 30 days [Fac10b].

Unfortunately it is the property of convenient communication and information sharing which gives rise to serious concerns with regard to users' *informational self-determination*. In general, user data is concentrated under one single administrative domain, and therefore, is subject to intentional as well as unintentional data disclosure. Of course, their exist users who do not care about disclosure of their profile data since they maintain and operate their OSN accounts for the sole purpose of profiling or even as an avatar. Nevertheless, plenty of users trust SNS providers to comply with their privacy and security statements ignoring the fact that no provider can guarantee for the integrity of the software system and all of its employees.

In contrast to such user preferences, many SNS providers attempt to aggregate centralized-accessible users' profile information to map and link their social dependencies into a single *social graph*. A social graph represents an extremely valuable knowledge base which allows for various data mining operations e.g. the derivation of individual preferences and habits. In a less critical scenario, such data may be utilized by third party providers in order to realize personalized product recommendation systems. Recently, Facebook announced exactly this kind of service as *social plugins* [Tay10]. Social plugins represent a novel possibility which permits third party providers to query Facebook by means of the *Open Graph Protocol* [Fac10a] for certain profile information in order to include personalized content into their websites. A rather serious situation is given in case an insurance company derives knowledge about users' sport activities, food patterns, or even personal indispositions from such a social graph. This information could be abused to estimate health hazards and risk for illness in order to increase costs for a certain insuree.

Since any SNS provider guarantees careful observance of its users' privacy requirements, one may argue that in reality such threats do not exist. However, recent past has shown that the threat of data leaks [Sec08], [Gro10], [McM10] as well as the unsolicited relaxation of OSN privacy settings [Nee09], [Ban09], [Car10] cannot be prevented. Even profile deletion represents a serious problem. Although OSN providers often offer the opportunity to terminate accounts [Fac10c], such deletion does not necessarily mean that each piece of content ever posted or uploaded to an OSN will dissolve [Ram08], [Wal09]. Such content distributes to other users' sites and is no longer under control of its author [KW09].

OSNs greatly support the dissemination and replication of any content (documents, email, and chat communication, forum threads, and the like) on the Internet. As a result, users lose control over and ownership of their content as

soon as they release it [Sch09]. Hence, a multitude of users does not only suffer from the threat of unsolicited profile disclosure and private data leakage, but also from increasing *social network pollution*. The reason for this must be attributed to sizable contact sets which often comprise several hundred contacts per user [Fac10b]. This increase is mainly driven by the fact that anybody is allowed to offer its friendship to anybody else. A multitude of such invitations are accepted without expressive knowledge about the originator. Personal information and content becomes available to a multitude of questionable contacts, a development, a user should never intend.

Focusing on aspects of mobile computing, we identify another problem users presently suffer from. A multitude of SNS and third party providers already offer context-aware applications for *Mobile Internet Devices* (MID). Such applications allow for the interaction with nearby users supported by profile information collected from an OSN. However, none of these software solutions support anonymous and secure contextualized communication, information aggregation, and information provision. A recent publication [BGH09] discusses this problem. In [BGRH09] the authors present a framework to enrich real-world location-based services with social network information without compromising user privacy and security. The proposed architecture allows location-based services to query a local area for social network information without disclosing a mobile user's identity. However, their solution does not solve privacy and security concerns, but shifts responsibility for sensitive data to a trusted third party.

In this paper, we present a hybrid and decentralized OSN design which aims on maximal compliance with privacy and security of its users' shared information. At the same time, our approach allows for minimal OSN pollution through undesirable linkage of OSN users. The main contributions of this work are *a)* a requirements analysis to support strong privacy and security for OSNs, *b)* a novel multi-domain design for a highly-available and decentralized OSN which complies with the elaborated requirements and *c)* a technical transformation of real-life communication patterns to an appropriate social network messaging design.

The rest of this paper is organized as follows. Section 2 provides a requirements analysis which forms the basis for the chosen OSN design. A scheme for secure communication and detailed description of the multi-domain OSN design are given in section 3. The technical transformation and integration of real-life communication patterns into our design are detailed in section 4. Section 5 discusses related work. Finally section 6 concludes the paper and gives an outlook on future work.

2 Requirements

Independent of the intended application one can identify several requirements an OSN must meet. In this work, we primarily focus on security and privacy. Though there has been some effort on the side of SNS providers to comply with privacy demands, applications such as *WhosHere* [myR10] or *Loopt* [Loo10] render them

useless. Both share social network identifiers over short range communication interfaces (Bluetooth, WiFi) and hence are not only able to aggregate user's profile information but also to enrich that aggregation with location information and technical details such as a MAC-address. Of course such aggregation results in even worse personal profile disclosure. In order to better understand the imminent necessity to turn away from present OSN developments, we define a set of requirements to which SNSs should adhere in order to *a)* better match the main idea of OSNs being a platform for private communication according to real-life communication patterns and to *b)* allow for secure and privacy-preserving data distribution and communication.

2.1 Informational self-determination

A centralized administration of OSN profiles and uploaded content is incompatible with a user's demand for informational self-determination. Even in case a trusted third party guarantees secure and confidential access to profile data and uploaded content, the problem of centralized administration, i.e. the opportunity for social graph derivation and abuse still exist. A completely anonymous and decentralized OSN cannot allow centralized hosting of sensitive data as well as the reliance on any kind of third party at all. As a presetting, informational self-determination requires that neither a user's profile information nor his personal content may be disclosed to any other than his trusted contacts. A user's trusted contact may have any means to determine a user's present physical anchor point in order to establish a confidential communication channel. All communication must guarantee safety against man-in-the-middle attacks. It must be possible for a user to configure fine-grained access to his profile information, i.e. we need a manageable and secure mechanism to publish a selected set of profile attributes, dependent on a trusted contact's identity. To give a user full control over its personal data, the possibility to permit trusted and selective profile access demands a simple and efficient revocation mechanism. This comprises a user's choice to cancel its OSN participation, and henceforth, deny future access to the content once published.

2.2 Strong trust relationships

Today, none of the prevailing OSN architectures reflects that kind of social relationships we are used to maintain in reality. This must be attributed to non-solicitous addition of unacquainted contacts and thoughtless disclosure of personal information. The process of establishing a new contact inside an OSN differs considerably from that in real life. In real life, trust heavily depends on the degree of acquaintance which is closely related to the kind of social links inside a social graph. Considering the personal behavior, one observes that, even in case a best friend recommends one of his best friends, we not necessarily share the same degree of trust for that person. Mapping these relationships to a social graph, a best friend represents a *one-hop relationship* whereas the best friend of

a friend (given that this person is not a friend of mine) corresponds to a *two-hop relationship*. To get back to the previous example, it seems to be rather questionable whether a person A shows another person D any trust at all in case the shortest social path between A and D is not a direct link. In the following, we use the term *chain of trust* to refer to all vertices on a path between two users X and Y (both included) inside a social graph.

We believe that it is exactly the process of incautiously making friends which causes huge (and therefore unmanageable) contact lists, unsolicited profile and personal information dissemination, and associated network pollution inside an OSN. As a major requirement, we limit the maximum length of the chain of trust to one-hop relationships. Consequently, it becomes almost impossible to arbitrarily search the OSN for unacquainted contacts. Nevertheless, as already mentioned before, a user should still be able to get into contact with his two-hop relationships. It should be stressed that the process of contacting a two-hop relationship must not violate the previously elaborated requirements for informational self-determination. Hence, a user must not publish a one-hop relationship's profile information which otherwise would violate his requirement for informational self-determination.

2.3 Profile availability

As aforementioned, to prevent social graph construction and abuse, it is indispensable to turn from a centralized to a decentralized OSN architecture. We believe that any kind of trusted third party cannot guarantee the requirement of informational self-determination as defined before. It becomes obvious that a decentralized infrastructure which complies with these demands requires each participant to administer his profile on his own. However, an OSN is worth nothing in case published profile information is not available. We need secure and privacy-preserving online publication and storage facilities in order to allow access to data while its owner is offline. Consequently, and in addition to our requirements of informational self-determination and strong trust relationships, we insist on permanent availability and authenticated accessibility of all users' profile information, even in case the user is not online.

2.4 Mobility support

At present, mobile and ubiquitous computing become reality. Consequently most SNS and other third party providers offer applications for the iPhone or any Android-based MID, in order to keep synchronized with an OSN. Unfortunately, most SNSs do not allow for real mobility support. Since mobile computing is subject to limited input and output capabilities, the utilization of a user's social graph and his context information at the same time represents the foundation for highly-personalized service provision. Though one cannot realize personalization without exposing private information to some service (or users), it is possible to limit the impact of information disclosure to a configurable granularity and

exchange only defined data between a restricted set of users. Mobile software also suffers from general problems related to network connectivity and computational power. Hence, mobility support for an OSN requires reliable communication which is based on a sophisticated infrastructure. Another essential requirement for our OSN platform represents its maximal support for mobile communication between a user and his one-hop relationships.

3 Concept and Design

In order to comply with all requirements identified in section 2, we decided to separate our architecture into three domains: a *social webspace*, a *social mobilespace*, and a *social homespace*. Figure 1 illustrates the components and their relationship from the user's view. Our design distinguishes synchronous and

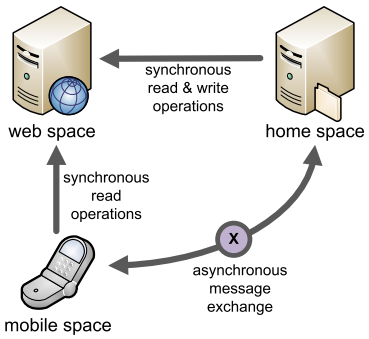

Fig. 1. User-centric visualization of the OSN domains. Entities of the social mobilespace are restricted to (synchronous) read-only operations on the social webspace. The social homespace has (synchronous) read and write permissions. Message exchange between social mobilespace and social homespace is bidirectional, asynchronous, and based on the concept of exchangers.

asynchronous communication. The mechanism for message exchange between entities of the social mobilespace and the social homespace allows for secure and asynchronous messaging between acquainted users. According to [Wer10], we decided to allow the usage of modern technologies such as strong encryption and some sort of microblogging to enable anonymous information exchange between users to the maximum extent possible. The social webspace is a passive system component and represents the main access point for identity information of a user. Among other data, this location holds information about a user's name, mailing address, email address, age, and marital status. To limit profile access to the corresponding user and his one-hop relationships only, this information is stored in a strongly encrypted way. The social homespace represents one of possibly many computing devices like a personal PC which provide access to an OSN. However, the social homespace differs from any other device in that

it is the only component allowed to modify a user's social webspace. The social homespace is responsible for the maintenance of all profile data of the user itself as well as profile copies and associated cryptographic keys of the user's one-hop relationships. The social mobilespace corresponds to any kind of MID a user can optionally register with the social homespace. A registration may result in proactive notifications in case the social homespace experiences profile updates. Although social homespace and social mobilespace significantly differ in connectivity, computing power, and power supply, it should be transparent to a user and his one-hop relationships, whether he is interfacing the OSN through his social homespace or his social mobilespace.

3.1 Secure Messaging

In order to comply with our requirements it is essential to base our OSN design on a secure and privacy-preserving messaging infrastructure. Since messaging between users of an OSN requires asynchronous communication, we decided to model our messaging scheme as an abstract channel which provides similar functionality as a mailbox. The proposed OSN messaging mechanism adopts the idea for *locagram* exchange as described in [Wer10].

Assuming an already established one-hop relationship, two users A and B possess a *link-specific* public key pair for exclusive communication with each other. This means that A is the only OSN participant which knows about the public key B has generated for exclusive communication with A, and B is the only OSN participant which knows about the public key A has generated for exclusive communication with B. The reason for our decision to generate a separate key pair for each directed edge of the underlying social graph is twofold: First, we achieve a reasonable degree of anonymity since it becomes computational expensive to derive a user's identity from its social link-specific public keys. Second, in case a public key is considered *compromised* [1], revocation can be simply performed by deleting the corresponding private key. In addition to a link-specific public key, a user A knows about the address of a link-specific communication channel, called *exchanger*, which provides the functionality of a mailbox for B. Such an exchanger could be realized through non-persistent technologies (e.g. IRC), semi-persistent public storage such as a microblog (e.g. Twitter), or fully persistent technologies (e.g. WebDAV). Dependent on the underlying technology, an exchanger can be addressed by a nickname, a channel name, or an URL. In case A wants to send a message to B, A encrypts its message based on B's link-specific public key (e.g. in accordance to PGP [Gar94]) and places the encrypted message together with the corresponding public key at B's exchanger. Dependent on the underlying system characteristics, B can fetch and decrypt all messages sent to his exchanger.

It should be stressed that a user can utilize multiple exchangers. In order to increase the computational complexity to determine user identities, a user even

[1] We consider a public key to be compromised in case any user C determined the identity of its creator.

could decide to announce a separate exchanger to each of its one-hop relationships. Furthermore, an exchanger can be used for asynchronous transmission of any kind of data i.e. A cannot only place messages but also arbitrary content at the exchanger of recipient B.

3.2 Social Webspace

The social webspace may be seen as a user's directory service which provides information about the user to his one-hop relationships. Due to the requirement for profile availability, the social webspace must be always online. Since a user's social homespace or social mobilespace cannot guarantee permanent availability, it must be possible to export this component to any third party webspace provider. Following our requirement for strong trust relationships, as a default configuration, we deny unencrypted publication of any kind of a user's personal as well as his one-hop relationships' information. Therefore, the social webspace holds a user's profile information, encrypted for each one-hop relationship based on the corresponding link-specific public key. Furthermore, it stores a user's one-hop relationship exchanger addresses for each entity (MID) of the user's social mobilespace domain, again based on the corresponding link-specific public key.

In order to support distinct access rights for different sets of users, we decided to encrypt one copy of the corresponding profile information for each one-hop relationship. In case of profile modifications, this necessitates re-encryption and re-publication of a user's profile data. However, we believe that this overhead is acceptable: In our privacy-enhanced OSN architecture the threat of OSN pollution no longer exists, and hence, a user maintains a severely reduced set of one-hop relationships i.e. profile data is not subject to frequent changes. In accordance to PGP, a profile could contain symmetric group keys for a specific application like a pinboard. Only in case the revocation of a one-hop relationship is required the asymmetric operations would have to be performed.

3.3 Social Homespace

The social homespace corresponds to a computing environment which is provided by the user itself. Although it should be transparent to a user whether he is interfacing the OSN through the social homespace or the social mobilespace, at present the social homespace represents the only entity which is allowed to perform modifications to the social webspace (read and write permission). In case a user changes certain profile information or decides to modify access rights for any one-hop relationship, the social homespace has to perform an update operation on the social webspace. Such an update comprises the re-deployment of all re-encrypted modifications. As we will see later, this necessitates an additional synchronization routine between social homespace and social mobilespace in order to keep a user's devices synchronized.

Dependent on the configuration of the underlying computing environment, a social homespace cannot only serve as a communication interface to the OSN,

but also as a personal storage for sharing content with the OSN. For instance, a computing environment representing the social homespace could consists of a personal desktop computer, a NAS device, and a ADSL-router. To enable communication between a user's one-hop relationships and his social homespace the social homespace must be addressable through a public IP address. Hence, a user's upstream network access device must allow for cone-NATed communication. In order to deny unauthorized access personal content must be subject to access control which reflects the trust relations published in the social webspace.

3.4 Social Mobilespace

Besides social webspace and social homespace our architecture includes the social mobilespace which is deployed at one or more of a user's MIDs. At present, it is very common that a mobile network provider does not assign public IP addresses to mobile phones. Therefore, the only solution to proactively establish a communication path with a user's social mobilespace is to provide the address of a well-known VPN-tunnel endpoint which is responsible for tunneling all traffic to the corresponding mobile device. As such a design does not comply with our demand for mobility support, we decided to use a pull-based messaging infrastructure which is built on the exchanger concept.

As it should be transparent for a user whether he is interfacing the OSN through the social homespace or the social mobilespace, both domains are subject to synchronization. To keep our design simple, we decided to restrict any modifications of the social webspace to the social homespace. In case the social homespace recognizes a pending update operation, it simply performs the necessary write-operations to the social webspace. To keep the social mobilespace in sync with the social homespace, a user which interfaces the OSN through his social mobilespace performs an interval-based read operation on his social webspace. In order to synchronize pending modifications which occur in the social mobilespace, the corresponding entity has to utilize our abstract channel to notify the social homespace about the pending adaptations. As soon as the social homespace becomes active, it has to apply the pending modifications to the social webspace.

4 Social Network Messaging

We decided to support two basic schemes to get into contact with another user, *a) out-of-band invitation* and *b) coupling*. In the following, we will discuss these mechanisms in detail.

4.1 Out-of-band invitation

In order to allow for the establishment of a new one-hop relationship between two persons A and B, our design provides for an email-based out-of-band (OOB)

mechanism. This mechanism can be easily mapped to other OOB channels. For instance, one could imagine the necessary information exchange between two *prepared* mobile devices based on NFC, Bluetooth, or QR-Codes. Prepared in this context means that both devices have the corresponding OSN software installed.

An OOB channel is needed to safely authenticate each other i.e. to satisfy our demand for strong trust relationships. The mechanism works as illustrated in figure 2. Users A an B agree on a password or a PIN (e.g. via phone). Then A sends an E-Mail to user B (1) containing a link to the OSN software, an exchanger address, a link-specific public key, and some explanatory text. This message may be seen as a weak authentication of user A, as we rely on email, a personal message, and well-established email spam filter mechanisms. To achieve complete safety against spoofing and replying of email messages, one could rely on secure end-to-end email e.g. in accordance to PGP. In case B is not a member of the

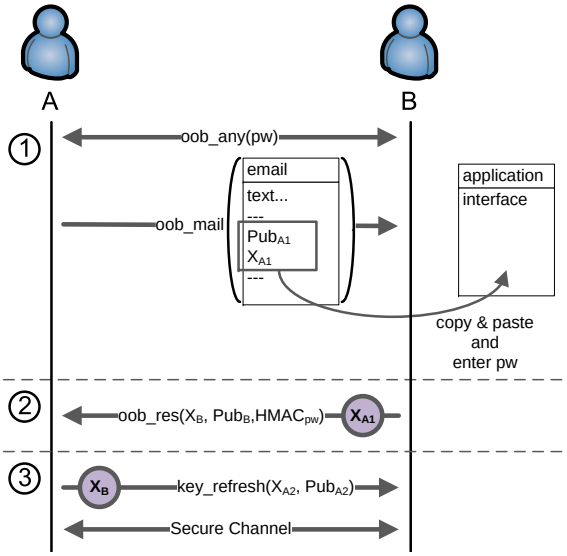

Fig. 2. The message exchange for out-of-band invitations.

OSN yet, B can follow the provided link and download/install the OSN software first. After B has started the software, the technical information included in A's email invitation (i.e. exchanger address and link-specific public key) can be copied to the corresponding dialog. To support copy-and-paste on the side of B, the invitation complies to an application-specific and e-mail compatible format. B will be prompted for the previously agreed password in order to verify the request. Now B can send a message to A including a freshly generated link-specific public key, an exchanger address, and an HMAC which is based on the previously agreed password (2). As the link-specific public key in the email cannot be considered to be secure, A will perform a key refresh operation (3) via the

secure channel established in (2). Finally, A and B have completely prepared for secure communication. As mentioned before, email-based invitation is a special form of OOB invitation. In a e.g. NFC-based MID-to-MID OOB invitation, step (1) would be performed in a secure environment without the threat of spoofing or replying attacks.

4.2 Coupling

In reality it is a common constellation that, after a person A has introduced two of its friends B and C to each other, B and C also establish a close friendship. In order to map this situation to our OSN approach, we integrate *coupling*, a simple mechanism which complies with the demand for strong trust relationships. Coupling supports the establishment of a new one-hop relationship between two users B and C which maintain a two-hop relationship via user A in advance. Figure 3 illustrates the simplified message exchange necessary for coupling. To

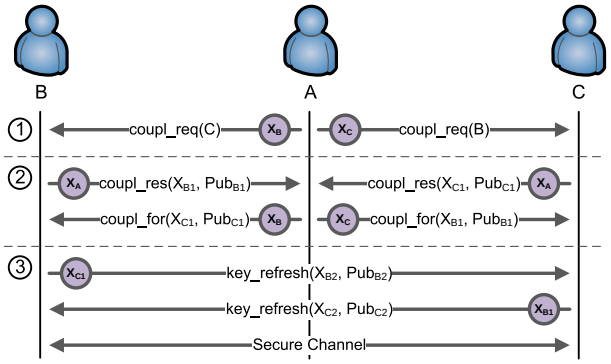

Fig. 3. A initiates the coupling of B and C.

initiate coupling between B and C, A sends a coupling request to B and C which optionally contains parts of the profiles of B and C which they have marked to be public (1). This could include a name or a list of personal interests. B and C can deny or accept this request. In case they accept A's offer, B and C each specify a link-specific public key and an exchanger address to be used during coupling. A will forward the re-encrypted messages (2). In order to comply with strong trust relationships B and C have to perform a key refresh (3) since A knows about the link-specific public keys applied during the coupling procedure.

5 Related Work

The idea to migrate from centralized to decentralized and personally operated OSNs is quite young. Therefore, there have not been published plenty of articles in this field yet.

Notable work has been published by Cutillo et al [CMS09b] [CMS09a] who present their OSN platform Safebook. This platform represents a decentralized P2P-based architecture which targets at users that request for compliance with their personal privacy and security demands. However, since their approach depends on the deployment of a DHT substrate, the authors cannot guarantee a 100% availability. A DHT also implicates additional management: it complicates the OSN protocol, it introduces additional signaling traffic, it cannot be operated without caching, and it suffers from a weaker trust model. In order to prevent well known impersonation and sibyl attacks [UPvS09], their approach necessitates a trusted identification service. However, such a certificate authority again represents a centralized third party instance which users of a decentralized OSN do not accept. The authors state, that this may be implemented offline, but do not explain how. Another critical point of their concept is, that any node may request access to a user's social network information (profile). That opportunity allows for indirect friendship requests which represents the foundation for OSN pollution. This also introduces a new order of complexity. To guarantee an uninterrupted chain of trust each request forward requires message decryption, signature re-calculation, and message re-encryption. Similar to our approach profile attributes are published encrypted. However, access in their scheme is group based i.e. key revocation an redistribution accounts for the notification of all friends about a new key for the freshly encrypted attribute.

The authors of [BSVD09] present PeerSoN, a P2P-based OSN system which aims on privacy relevant issues like authentication, encryption, and the prevention impersonation attacks. Peers need not be connected to the Internet in order to make use of their social network. However, this usage is restricted to insight communication with other PeerSoN enabled devices and does not hold for OSN users that want to access user profile data. Since their system offers a DHT-based lookup service, previously discussed problems still exist. Another assumption made by the authors is the availability of a GUID (e.g. an email address). In a privacy enhanced network it should be the choice of a user whether to publish his email address or not. Even hashing does not assure complete anonymity as a node which is requested several times for one and the same hash, may derive certain information about a certain user.

The authors of [GTF08] do not develop a completely novel OSN architecture, but attempt to integrate some privacy features into present SNSs like Facebook. They propose an anonymity scheme which builds on pseudorandom substitution. Based on dictionaries, each piece of encrypted private data becomes substituted by a pseudorandom cipher. This approach shares our idea to encrypt little pieces of information instead of an entire profile in order to allow for fine-grained access to a user's personal properties. However, considering their proposed key management, it becomes obvious that their scheme depends on an additional communication channel like a trusted third party's PKI in order to allow for sufficient security.

The authors of [SVCC09] and [SLCC08] follow a DHT-based organization of social information. However, their concept of virtual individual servers (VIS)

does not meet the privacy and security demands of a decentralized OSN as administrative tasks are shifted from the centralized OSN to a centralized VIS provider.

Lockr [TSGW09] targets at the improvement of privacy for centralized and decentralized online content sharing services. To some degree, this system shares some similarities with our approach since it distinguishes between the management of social relationships and shared content. It aims on enhancing privacy and accelerating content sharing. However, Lockr only reduces the chances for mismanagement or accidental disclosure of social networking information. Compared to our approach, Lockr still allows users to map content which is shared among traditional OSNs like Facebook to their anonymous OSN identity. Although each platform is mapped to a pseudonym, it is possible to correlated pseudonyms by usage and activity analysis. This allows for the collection of information about one and the same user in different OSNs. Our solution prevents such attacks as content is always hosted encrypted or can only be downloaded in case a secure session has been established in advance.

6 Conclusion

In this paper we presented a requirements analysis for a secure and privacy-enhanced OSN. With these requirements in mind, we developed a novel OSN design which is based on the separation of an OSN into the three domains *social webspace*, *social homespace*, and *social mobilespace*. This distinction as well as the decentralized administration of all domains allows for strict compliance with our demands for permanent *profile availability* and *mobility support*. In addition, our implementation for the establishment of new relationships ensures adherence with our requirements for *informational self-determination* and *strong trust relationships*.

Thanks to the increase of computational power and storage on the Internet and Mobile Internet Devices it is possible to utilize strong cryptographic algorithms to allow for secure information exchange. In combination with the increasing count of always-online infrastructure in the private area it is possible to remove the need of a central platform for an OSN. As this process is still ongoing we propose to use a web-server as a reduced mirror of the encrypted information of the homespace such that the social network will work as expected even in case of disconnection of the homespace.

References

[Ban09] Kevin Bankston. Facebook's New Privacy Changes: The Good, The Bad, and The Ugly. online, December 2009. http://www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly.

[BGH09] Aaron Beach, Mike Gartrell, and Richard Han. Solutions to Security and Privacy Issues in Mobile Social Networking. In *CSE '09: Proceedings of the 2009 International Conference on Computational Science and Engineering*, pages 1036–1042, Washington, DC, USA, 2009. IEEE Computer Society.

[BGRH09] A. Beach, M. Gartrell, B. Ray, and R. Han. Secure SocialAware: A Security Framework for Mobile Social Networking Applications. Technical Report Technical Report CU-CS-1054-09, Department of Computer Science, University of Colorado at Boulder, June 2009.

[BSVD09] Sonja Buchegger, Doris Schiöberg, Le Hung Vu, and Anwitaman Datta. PeerSoN: P2P Social Networking - Early Experiences and Insights. In *Proceedings of the Second ACM Workshop on Social Network Systems Social Network Systems 2009, co-located with Eurosys 2009*, 2009.

[Car10] Nicholas Carlson. WARNING: Google Buzz Has A Huge Privacy Flaw. online, February 2010. http://www.businessinsider.com/warning-google-buzz-has-a-huge-privacy-flaw-2010-2#click-into-buzz-on-gmail-1.

[CMS09a] Leucio Antonio Cutillo, Refik Molva, and Thorsten Strufe. Safebook: Feasibility of transitive cooperation for privacy on a decentralized social network. In *WOWMOM*, pages 1–6, 2009.

[CMS09b] Leudo Antonio Cutillo, Refik Molva, and Thorsten Strufe. Privacy preserving social networking through decentralization. In *WONS'09: Proceedings of the Sixth international conference on Wireless On-Demand Network Systems and Services*, pages 133–140, Piscataway, NJ, USA, 2009. IEEE Press.

[Fac10a] Facebook. Open Graph protocol. online, Mai 2010. http://developers.facebook.com/docs/opengraph.

[Fac10b] Facebook. Press Room. online, April 2010. http://www.facebook.com/press/info.php?statistics.

[Fac10c] Facebook. Privacy: Deactivating, Deleting, and Memorializing Accounts. online, April 2010. http://www.facebook.com/help/?page=842.

[Gar94] Simson Garfinkel. *PGP: Pretty Good Privacy*. O'Reilly Media, November 1994.

[Gro10] Jennifer Van Grove. Blippy Users Credit Card Numbers Exposed in Google Search Results. online, April 2010. http://mashable.com/2010/04/23/blippy-credit-card-numbers/.

[GTF08] Saikat Guha, Kevin Tang, and Paul Francis. NOYB: privacy in online social networks. In *WOSP '08: Proceedings of the first workshop on Online social networks*, pages 49–54, New York, NY, USA, 2008. ACM.

[KW09] Balachander Krishnamurthy and Craig E. Wills. On the leakage of personally identifiable information via online social networks. In *WOSN '09: Proceedings of the 2nd ACM workshop on Online social networks*, pages 7–12, New York, NY, USA, 2009. ACM.

[Loo10] Loopt. Loopt. online, May 2010. http://www.loopt.com/.

[McM10] Robert McMillan. 1.5 Million Stolen Facebook IDs up for Sale. online, April 2010. http://www.pcworld.com/businesscenter/article/194843/15_million_stolen_facebook_ids_up_for_sale.html.

[myR10] myRete. WhosHere. online, May 2010. http://myrete.com/whoshere.html.

[Nee09] Rafe Needleman. How to fix Facebook's new privacy settings. online, December 2009. http://news.cnet.com/8301-19882_3-10413317-250.html.

[Ram08] Anita Ramasastry. On Facebook Forever? Why the Networking Site was Right to Change its Deletion Policies, And Why Its Current Policies Still Pose Privacy Risks. online, February 2008. http://writ.news.findlaw.com/ramasastry/20080229.html.

[Sch09] Bruce Schneier. Architecture of Privacy. *IEEE Security & Privacy*, 7(1):88, 2009.

[Sec08] The H Security. Facebook fixes data leak. online, July 2008. http://www.h-online.com/security/news/item/Facebook-fixes-data-leak-736509.html.

[SLCC08] Amre Shakimov, H. Lim, Landon P. Cox, and Ramon Caceres. Vis-à-Vis:Online Social Networking via Virtual Individual Servers. Technical report, Duke University, May 2008.

[Smi09] Justin Smith. Facebook Now Growing by Over 700,000 Users a Day, and New Engagement Stats. online, July 2009. http://www.insidefacebook.com/2009/07/02/facebook-now-growing-by-over-700000-users-a-day-updated-engagement-stats/.

[SVCC09] Amre Shakimov, Alexander Varshavsky, Landon P. Cox, and Ramón Cáceres. Privacy, cost, and availability tradeoffs in decentralized OSNs. In *WOSN '09: Proceedings of the 2nd ACM workshop on Online social networks*, pages 13–18, New York, NY, USA, 2009. ACM.

[Tay10] Bret Taylor. The Next Evolution of Facebook Platform. online, April 2010. http://developers.facebook.com/blog/post/377.

[TSGW09] Amin Tootoonchian, Stefan Saroiu, Yashar Ganjali, and Alec Wolman. Lockr: better privacy for social networks. In *CoNEXT '09: Proceedings of the 5th international conference on Emerging networking experiments and technologies*, pages 169–180, New York, NY, USA, 2009. ACM.

[UPvS09] Guido Urdaneta, Guillaume Pierre, and Maarten van Steen. A Survey of DHT Security Techniques. *ACM Computing Surveys*, 2009.

[Wal09] Chris Walters. Facebook's New Terms Of Service: "We Can Do Anything We Want With Your Content. Forever.". online, February 2009. http://consumerist.com/2009/02/facebooks-new-terms-of-service-we-can-do-anything-we-want-with-your-content-forever.html.

[Wer10] Martin Werner. A Privacy-Enabled Architecture for Location-Based Services. In *MobiSec '10: Proceedings of the Second International ICST Conference on Security and Privacy in Mobile Information and Communication Systems*, Catania, Italy, 2010.